(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 703 094 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
27.03.1996 Bulletin 1996/13

(21) Application number: **95908943.4**

(22) Date of filing: **20.02.1995**

(51) Int. Cl.[6]: **B42D 15/10**, G06K 9/46

(86) International application number: **PCT/ES95/00021**

(87) International publication number:
WO 95/25640 (28.09.1995 Gazette 1995/41)

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(30) Priority: **21.03.1994 ES 9400595**
26.05.1994 ES 9401171
05.07.1994 ES 9401452

(71) Applicant: **I.D. TEC, S.L.**
E-28761 Tres Cantos (ES)

(72) Inventor: **COBIAN SCHROEDER, Carlos**
E-28046 Madrid (ES)

(74) Representative: **Ungria Lopez, Javier et al**
Avda. Ramon y Cajal, 78
E-28043 Madrid (ES)

(54) BIOMETRIC SECURITY PROCESS FOR AUTHENTICATING IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNATION

(57) The security processes and products are based on coded topological and/or biometric information. Coded topological data, corresponding to a security document comprising an image, may be printed on the document in order to the used for its authentication. It is thus possible to establish a relationship between an image and certain pattern features contained in a database, said relationship being used for the fabrication and authentication of security documents and for the facial recognition of individuals.

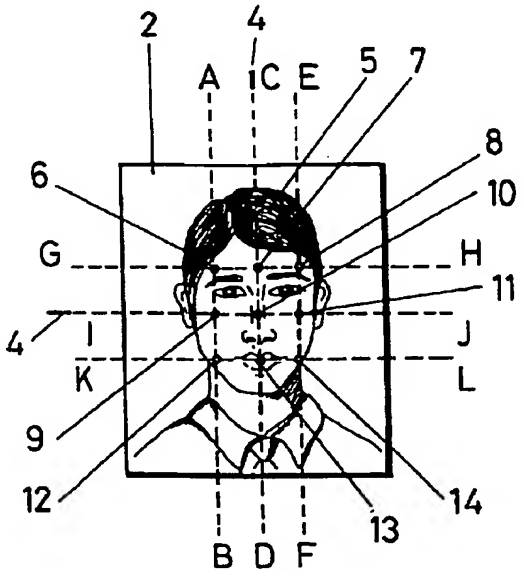

FIG. 2

EP 0 703 094 A1

Description

OBJECT OF INVENTION

This invention, as described in the presentation of this descriptive report, refers to a biometric security system and authentication of identity cards, visas and passports, as well as the face identity of the holder, whose purpose is to provide these identification documents with univocal elements of identification and validation which will allow both the holder and these identity documents to be authenticated as genuine or false, if they have been fraudulently reproduced or handled, changing or replacing the identity, personal characteristics or face image.

To obtain this end a security or validation system has been designed, printing certain colored lines on the identity document in the form of a grecque or filigrees which in a coded and univocal manner represent the topology of the actual card or identity document in its most sensitive parts, so that when any attempt is made at reproducing or forging these identity documents, this fraudulent reproduction or handling is clearly and irrefutably revealed.

The security validation which is object of the invention is based on a double application in this proposal. First of all points are taken at random on the identity card or document using a parameter algorithm. The choice of these points will depend on parameters such as, for example, the birthdate of the holder, with will thus individualize the choice of these points by means of a scanner which analyses the colour of each point or its tones of grays, where these values are numerically coded and in turn assigned an equivalence to a specific colour. With this numeric or colour code which is printed on the card in the form of a grecque or filigrees of colored lines, an univocal code of the card or identity document is formed.

In addition, the formation of a data base of master/pattern features is also object of the invention, which closely applies to the authentication of the individuals and their identity documents or cards, where, by comparing the zones of the face features, a synthetic image of the individual can be obtained by adding the basic features that are taken from the data base on master/pattern features, which in turn allows a numeric code to be made and a translation into its equivalent colour code, so that, from what has been explained above, this numerical code or the colour line grecque is printed on the card or identity document as validation, completed with the additional coloured lines that code the date of birth, christian name and surname with their first initials or in full.

The invention makes it possible to use and make the two validation modalities compatible in one and the same top security identity document or card, and also the face identity of the individuals who are the holders of these identity documents.

Closely related with the authentication of individuals and their identity documents or cards, a data base of master/pattern features is formed where by comparing the areas of the face features, a synthetic image of the individual can be obtained by adding the basic features that are taken from the master/pattern features data base, which in turn allows a numeric code and translation in its equivalent colour code, and, as mentioned above, this numeric code or the grecque of coloured lines is printed on the identity document or card as validation, and this is completed with the additional coloured lines which code the date of birth, christian name and surnames with their first initials or in full.

To procure maximum security in the production of these documents, the invention foresees that the document in question embody some special covers on which all the safety validations relating to pigments will be printed directly, and also all the colour codes or filigrees, on the extrusion on their inner polyolefin or polypropylene or low density polyethylene face and in this way, likewise all the holder's personal data, face image that is obtained from the scanning and digitalization of the photo which the holder submits for each identity document, along with the print of the holder's latent face image or of the holder's synthetic or composed face image.

ANTECEDENTS OF THE INVENTION

There are a great deal of production systems and technologies for identity cards and credit cards, visas and passports, on all sorts of paper and plastic supports, and also based on photographic technique or on transfer of the holder's image by digitalized impression, using micro-bubble jet injection printer or thermal-sublimation or by photo-electrostatic or electro-photographic impression.

All the makers of these identity documents or of the elements which form them have placed great emphasis on the fact that the fraudulent handling of these identity documents be made more difficult, and that the defoliation or separation of the layers that form a card or document for a fraudulent or criminal alteration should cause the irreversible destruction of the whole of the identity document so that it cannot be recomposed with another identity/personality other than that of the holder for which this identity document or card was legally issued.

The market also contains a wide offer of phosphorescent and fluorescent pigments to be incorporated on the layers that form these identity documents or cards, which efficiently render any attempt at photocopying original documents that have been manipulated to obtain a different identity to that of the holder, result in a reproduction where the original colours have ostensibly changed, and in this manner the fraudulent reproduction is avoided.

However, the present state of the art of high resolution colour digitizers and scanners today allows any sort of original document to be reproduced with very high colour definition printers, which are difficult to distinguish from the original by pixel to pixel exploration and sidestepping the distortion effect of the fluorescent/phosphorescent pigments which disguise the result of the

reproduction, by illuminating the original which is to be reproduced using a light that is filtered on the wave length on which this pigment is enabled.

The biometric validation methods have until now hardly been used at all in both security and as means of authenticating the card holder or identity document holder and of the actual card as genuine or forged/manipulated.

Moreover, neuronal network systems are now available on the market to identify pattern, and also fuzzy logic technologies.

The major drawback of neuronal networks to generically identify any kind of pattern, available on the market, lies fundamentally in the fact that once the pattern that are to be identified have been defined, the system is then practically closed or incapable of recognizing any other new pattern which we wish to introduce, because depending on the complexity of the new pattern, the entire system must be restructured and reorganized in what is known as a "system training process", with a great loss of time. Translating this circumstance and characteristic to a face identity use means that every time a new face of an individual must be introduced in the data base of this specific person's particular features, the other the data base of features of other specific individuals must be restructured in this "system training process". This operation may take a few minutes when this is used to identify a couple of hundred faces of individuals. When this technology has to be used for groups of hundreds of thousands of individuals or millions of faces in what can be called "population system" use, it is not practical because it takes too long to reorganize and to recognize the features.

DESCRIPTION OF THE INVENTION

The procedure of this invention has been designed for the reasons that we have explained in the above chapter, and it foresees security validations and authentication of the actual identity card or document, as well as the holder. The procedure is also biometric and can be used in the authentication of each individual who forms a community within a population census or register data process system.

To have reliable references when determining the authenticity or falseness of an identity card or an identification document, and consequently its holder, we must establish a number of significant points that are univocally chosen, that is to say, based on the card's own parameters and on the identity of its holder and procure the numeric significance of these points, depending on both the topological nature of the identity card or document and on the biometric type, in other words, depending on the face features of the holder's face image which is transferred on the card, and print the significance or equivalence of these topological or biometric points in numeric code or colour line on the card, so they form part of its information or of the identity document in an unalterable way and in an univocal relation unknown, logically, to any presumed or possible forgers of such documents.

In respect of the data base of master/pattern features, this foresees a comparison of the zones of the face features and a synthetic image or robot face image of the individual to be obtained by adding basic features taken from this data base, which in turn allows a numeric code and a translation in their equivalent colour code; this numeric code or grecque of colour lines are printed on the identity document or card as validation and are completed with the additional colour bars or lines which code the date of birth, christian name and surnames, with their first initial letters or in full.

Another characteristic novelty is to proportion the document with an additional validation which will consist of printing the latent image that is obtained from the face or photographic image of the holder, or else from the impression of the holder's latent face image where the original features have been replaced by others which are most similar to and coincide with the respective master/pattern features contained in the data base of reference master/pattern features of the data process system.

In addition, it is object of the invention to print, when applicable, the composed face image or synthetic image taken from the original photograph of the holder on these identity documents, cards, visas and passports, using the systematic analysis of features, extraction of characteristics and their parametric/anthropometric points.

BRIEF DESCRIPTION OF THE DRAWINGS

To complete the description which we are going to give below, and to help understand better the characteristics of the invention, a set of drawings is enclosed with this descriptive report, which will be used to offer an easier explanation of the innovations and advantages of the invention procedure.

Figure 1.- Shows a reference configuration of an identity document, credit card, visa or passport, where the face image of the holder is located, and the real or virtual window of the colour code.

Figure 2.- Shows a view of the possible significant points of the card which can be selected for a numerical code and their translation on coloured line, concentrating the selection of these points on the holder's photograph.

Figure 3.- Shows the configuration of the real or virtual window of the translation on coloured line of the numerical code number arising from significant points of the card and also the master/pattern features which match the holder's face image.

Figure 4.- Shows a possible face segment from which to take master features which can be used as reference to form a data bank on master features, which in turn and based on this face segment would analyze each basic feature of each individual and find their equivalence in the master/pattern features base, using the data base system for face identity per computer/work station.

DESCRIPTION OF THE PREFERRED FORM OF EXECUTION

Based on these figures, and specifically referring to figure 1, a possible optional configuration of a card 1 can be observed, identity card, credit card, visa or passport, where there are pre-printed coloured ink security filigrees, and where the face image 5 has been transferred by any procedure, whether photographic or printing by heat transfer/sublimation, or by colour printing of micro-bubble jet injection or by means of electro-photographic colour, on zone 2, of the holder of the card or identity document. In addition the personal data 5' of the holder are printed on the identity document or card. The coloured line code window 3 is determined and located anywhere on the card. By way of example, it has been chosen just above the face image 5 of the holder, also foreseeing the printing of some marks 5 or references for centering the scanner/video camera of the face image, and for selecting significant points of the card.

Once the nucleus 1 of that card has been produced, with all its elements as explained in figure 1, this card, and in particular the face image or photo 5, is digitalized using a scanner/video camera with CCD coloured image or line connected to a personal computer, where a prefixed and secret algorithm is fitted, which can be personalized by parametrizing for each identity card, for example, using the holder's birthdate as personalized parameter.

This description will describe the possibility of one of the multiple algorithms for selecting significant points of the card, with the help of figure 2. In this figure, the horizontal and vertical marks 4 can be observed, such that the computer, with the help of the algorithm, will virtually plot lines C-E and I-J as central reference lines and although these are located precisely in the same place for all cards, they will cross the different face images of the other cards at different zones. The computer will also plot the other lines A-B, E-F, G-H and K-L, in terms of a distance that will be calculated between given limits which can be determined in a maximum range of several millimeters and following the birthdate parameter, so that the distances between lines will be different in one identity card and another. The points of intersection that are obtained from these lines, which have been given the reference numbers 6, 7, 8, 9, 10, 22, 12, 13 and 14, will also be different in one identity card and another, with the peculiarity that other points can be chosen with the cross-section of circles and straight lines, for example.

Depending on the type of scanner/video camera that is used to explore and digitalize the face image of each card holder, a characteristic colour and its tones or grays and its shades can be established, with up to 256 tones in both cases, for each point that is chosen. This characteristic colour, that is attributed to each point that is chosen or scale of grays when the face image is in black/white, allows a numerical code for each point: for example, the international PANTONE colour numeration or any other that can also be applied as secret mode. This numeration of the selected points can be printed on the card, or else the equivalent colours in the form of a coloured line grecque, forming the real or virtual code window 3, printing with a printer that is connected to the personal computer as reported above, with a logical printing on card 1 in the manner that is given by way of example in figure 3.

The real or virtual code window 3 is printed with significant lines 15 in different colours, depending on its topological position, and each one represents the identification weight or colour or grey tone of points 6 to 14 that are selected. The window code is completed with lines whose different colours represent the christian name and surnames or initials, and also the birthdate. The filigrees or grecques of this window code are completed with neutral lines 16 which separate the significant coded lines 15.

Window code 3 whether really marked on card 1 or virtually windowed, must be of suitable dimensions to allow the scanner/video camera to have redundant information about each significant line of the grecque so it can discriminate the colours with absolute precision. The recommended dimensions are for a length of approximately 2.5 cm and a height of 2.5 to 3 mm.

The code that is contained in the grecque with lines of window 3 or the equivalent numbering that is printed on the card, is a univocal means of authentication of its face image and of the actual card, so that its holder is thus authenticated.

It is then only necessary to run the reverse process, that is to say, the code grecque of window 3 that has been explored by a scanner/video camera or directly the equivalent numerical code when this is printed on the identity card, is compared with the one that is directly obtained in the choice of significant points by the scanner/video camera that is connected to the personal computer, by means of the parametrizable algorithm, so that when the birthdate is introduced via the keyboard, this should coincide with the numeric code 100%, thus validating and authenticating the holder and its identity document or card. If this does not coincide, this means that the holder's photograph or image has been substituted or manipulated.

The biometric modality of the invention is based on the use of a system of neural networks which will identify those which are today available on the market, but which are specifically adapted as is explained below for the patent purpose.

The formation of a facial recognition system which is object of this patent, is based on a scanner/video camera of CCD line or image, black/white or colour connected to a data process work station or a very powerful personal computer which in turn is connected to a high resolution colour printer, which may be micro-bubble or ink-jet injection , heat transfer/sublimation or photoelectrostatic/electrophotographic transfer. The generic program of identification of pattern based on fuzzy logic/neural networks is located at the personal computer/data process work station.

According to this invention then, the way that this technology is used, which is so practical and accurate in identifying generic patterns is modified, in the practical manner that is explained, with a specific end which is to reach the authentication of identity documents and cards and of the holder of each one, within a computerized population system.

It can be observed from figure 4 that the face image of the generic individual is divided up into different face zones, where the basic and fundamental features of any face are contained relating to hair 17, or forehead 18, or eyes and eyebrows 19, nose and ear 20, mouth 21 and chin 23, and also neck 22. In addition, and in the same way as the police "composite image" systems act by classifying the faces in a generic way, according to the anthropomorphic characteristics, these zones are in turn reclassified depending on whether this is a big-boned, round, triangular face, etc.

This criterion is established and introduced in the data process system as initial basis of comparison or reference as basic features. The comparison criteria is then introduced in the neuronal fuzzy logic network with successive face models to allow the system to distinguish which generic features of the real individuals are different, so that these features, within an ample group of real faces, either taken from photographs or video-images, or live, can be considered master/pattern features.

The system which is thus formed with hundreds of thousands of faces and millions, if possible, depending on the extent of the nature of the final use which is wanted, is fed with the scanner/video camera.

The personal computer/data processing work station, with this comparison criteria exclusively takes just a 75% of the features that pertain to the segment that is established from each real face, so that no real face, at the end of the process, is contained in the data base of master/pattern features of the system.

In a lengthy process, the data process system compares these face zones exhaustively with one another and establishes which features in each zone of the face and each individual are precisely the same or very similar and which are different in the whole and which are obtained as different zone features within the entire unit that is analyzed, passing on to the master features base or reference features.

The process can be repeated with faces of groups of individuals of different races and attire and modalities, for example, with glasses of one kind or another, with beard in one form or another, with one hairstyle or another, etc., which enrich the data base of master/pattern features of the system, which can cover over a thousand dozen different types.

Each master/pattern feature in black and white or colour is given a specific number within this data base of master features, and the system which is then formed is a facial recognition system with which a number of practical uses are obtained, which form part of this invention and which are explained below.

Any individual that is issued a card or identity document or credit document has his/her face image that is contained in the card digitalized with the scanner and also, if possible, live with video camera, so that the data process system can analyze the face segment comparing the resulting feature with the master/pattern features contained in the master/pattern features data base of the system. This on the one hand obtains a synthetic face image which characterizes and identifies this individual and which is represented on the monitor of the system computer in black/white or colour, and also obtains a numeric code which univocally characterizes this individual who is the card holder or holder of the identity document.

It has been explained above that the numeric code or its equivalent in coloured line code, is printed directly on the identity document or card in the form of window 3, with real or virtual frame, forming the coloured grecque which has already been described. Printing is done by the printer which is connected to the personal computer/work station of the system or face identity.

Also, the numeric code or numbering or the coloured line grecque of code window 3, printed on the card, allows the authentication of the card and its holder. Other coloured lines have been added to the coloured line code on the grecque which code the christian name and surnames, and also the holder's birthdate.

This numeration or equivalent of coloured lines of the grecque of window 3 is thus digitalized using scanner/video camera and is compared with the code result when the computer analyses with its face identity system, the features of the photo or face image of the card with the master features that are obtained, taken from the data base on master features. When this comparison coincides completely, this shows that the card is genuine and that its face image thus authenticates the holder.

As side-product of all this process which also forms the object of this invention, there is the possibility of extending the facial recognition live, that is to say, using video camera via digitalized photography with scanner, both connected to the computer of individuals who form part of a determinate group whose factions/features have been analyzed and a numeric code of the master/pattern features which identify and characterize them has been obtained, and which is contained in a data base on population or individuals wanted by the police, etc.

In accordance with the improvements of the invention, the photograph of a face image is suitably digitalized by scanner/video camera, obtaining a virtual black/white face image with 64 to 256 grey tones. The resulting virtual image is then explored internally with the specific data process program, to detect the horizontal zone which provides the maximum frequency of information. A Sobel operator or gradient and the like is then applied on the same virtual face image that has been obtained, using a determinate threshold of grays, obtaining a direct new virtual face image with the respective contours-edges of the face and the resulting factions/features of the eyes, nose, mouth and chin, where applicable. The

computer determines the center point of the eyes and measures the length and width and also the position of the eyes, nose, mouth and chin, where applicable as anthropometric parameters.

In addition, the characteristics which distinguish the face features are extracted with a specific data process program, so that the value of each pixel, in terms of the intensity of grays inside the rectangle of the selected information where the eyes, nose and mouth are described, is compared with a reference threshold, making the comparison with this data process program. The spacial composition and distribution of intensity of grays is also determined with fuzzy logic/neural network technology, obtaining space values with respective representation of vectors.

The master/pattern features contained in the reference data base are submitted to the same process that has been mentioned above, so that from each master/pattern feature, the respective characteristic anthropometric parameters and spacial values will be obtained and the respective vectors, all of this to allow the comparison of the features taken from any photograph of treated face image, to be established with regard to eyes, nose, mouth and chin, obtaining the equivalent master/pattern features in the reference data base which offer the most coincidence or similitude in respect of the initial face image.

These master features are likewise printed on the identity card or document in question, where the numeric code or colour code is also printed which corresponds to the selected master/pattern features, and where printing is performed with the respective printer that is connected to the system computer.

The computer program of the computer identifies the corresponding angle and distances of almost 50 to 100 most significant anthropometric points, depending on the type of face image, the edge or contour of the face relating to the center point between eyes, so that with these distances and their respective angles, a complete parametric code is obtained of the face image corresponding to the face in the initial photograph, by means of 400 to 600 characters (bytes), such that these parameters which differentiate the face image are transmitted by the computer which has generated them; this transmission can be performed on conventional telecommunication lines to another computer located at the other end of the same transmission line, and this receiver computer receives these characteristic parameters base from which it faithfully reconstructs the initial face image, all based on the fact that this receiver computer has also available the same data base of master/pattern features from which it obtains the master/pattern features relating to eyes, nose and mouth, corresponding to the code that is contained in the parameters that are received.

In addition, the document in question is provided with an additional validation which consists of printing the latent image derived from the face or photographic image of the holder, or else printing this latent face image where the original features have been substituted with those which most ressemble and coincide with the respective master features contained in the data base of reference master features of the data process system.

In addition, the printing, where applicable, of the composed face image or synthetic image derived from the original photograph of the holder on these identity documents, cards, visas and passports is object of the invention, applying the systematic analysis of features, extracting characteristics anthropometric parameters and their parametric points.

Latent face image is defined as the image obtained by digital scanning of the original photograph of the holder of the identity documents, visa, passport and which is synthetically printed in various colours or, preferably in just one colour, where the objective is to highlight the identity and similarity of this latent face image with the original, on these identity documents, because this is a duplication on these documents.

The object of the invention furthermore consists a transparent polyester cover on whose inner face there is printing with reflector pigment ink and ink visible under UV light, and also the printing of a frame. On this same inner face an electric discharge is applied, followed straight away by hot deposit extrusion of a layer of low density polyethylene or polypropylene so that a fine sheet of copper or aluminium or else non-thermo-laminate plastic is applied ob this surface that is formed, and this sheet will be affected by complementary windows or spaces which coincide with the printed frames on this transparent polyester cover, all prior to performing a crown electric discharge, immediately after which a hot deposit of low density polyethylene or polypropylene is performed, optionally with mixture of collagen/gelatine, to absorb water soluble ink.

The sheet of copper, aluminium or plastic is then removed, and an impression of ink, grecques, coloured filigrees, personal circumstances and also face image, latent face image and/or composed face image or derived synthetic face image is made on the last surface and directly.

In addition, on this same surface and by way of an option, also in a specular manner, these face images colour filigrees, etc., are printed, with either electrophotographic printing or else photoelectrostatic printing, and even by conventional printing.

As for the document in question, the nucleus of it will be formed on white paper or else white polyester or any other sort of white plastic or white printing and by way of an option it will include continuous printing lines, with the peculiarity that an electric crown discharge is applied on both sides, followed immediately by hot extrusion of low density polyethylene or polypropylene, with complete hot thermo-lamination with the personalized covers as defined above.

Claims

1. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT**

CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION, which is based on the nucleus or support of an identity document or card, with coloured lines in the form of grecques or filigrees, and also the respective personal data and circumstances and with the face image of the holder transferred on it, and supported by the use of a color image CCD or a line color CCD scanner/video camera connected to its respective computer, essentially characterized because an exploration is done by means of the scanner, partially or completely digitalizing the surface of the identity document or card, where the computer, which embodies a parametrizable algorithm, selects a sequence of points according to aleatory parameters for each identity document or card, where this computer runs an analysis for each point chosen, of the colour tone of each point taken from the surface of the card including their face image, and where each selected point with its colour tone is likewise assigned a numerical code where, either as numerical code and printed on the particular card, or in the form of coloured code lines, forming a grecque or filigrees the form of a frame or real or virtual code window on the actual card or identity document, this printing is performed by means of the colour printer connected to the computer, based on a thermal transfer/sublimation technology or by colour ink injection, electro-photographically or by digital photography; with the peculiarity that the christian name, surnames and birthdate are also coded in their equivalence to the respective colour code and printed on the real or virtual code window.

2. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claim one, characterized because an exploration is made by scanner and the digitalization of the lines of the grecque of the real or virtual window of the card code is performed, comparing with the parametrizable algorithm located in the personal computer, whether the set of significant points selected for this card coincides in their resulting numeric code with the equivalent code of the colour lines of the grecque contained in the real or virtual code window, showing the authenticity or falseness of the card, visa or passport.

3. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with the above claims, characterized because a data base is formed of master/pattern face features, which is used by way of reference to compare, code and identify faces, by means of a scanner / video camera in black/white or colour with image CCD or line CCD connected to the computer, which embodies a program based on neural network or fuzzy logic or image process technologies which distinguishes the differentiating features from among thousands of faces in photograph or in video image, extracting the common ones as master/pattern reference features of this set or population of faces, assigning each master/pattern feature a fixed and univocal colour code and a numeric code.

4. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with the above claims, characterized because an analysis is performed by scanner/video camera, of the face features corresponding to the face image contained in the identity document or card, where the computer runs an analysis of the basic features of this image, comparing them with the master/pattern features of the data base and obtaining a number of master/pattern features which form on the terminal-screen a synthetic characteristic image of this individual and where the printer that is connected to the computer prints on the virtual or real code window, the coloured lines in the form of grecque or filigree, which univocally characterizes the holder of this identity document or card; it is furthermore foreseen that as an option the consequent numerical code can be printed.

5. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with above claims, characterized because there is a digitalization by scanner of the real or virtual code window, the code lines of the identity document or card, from whose analysis the computer establishes the equivalence of the coloured lines with the respective master/pattern features, and it also decodes the christian name, surnames and birthdate, where the synthetic face image corresponding to these master features is represented on the screen of that computer, and where the synthetic face image should coincide with the face image of the identity document or card, and with the face of its holder.

6. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with above claims, characterized because a comparison is made by computer of the live image taken of each individual, by means of video camera, regarding the basic face features of that individual with the master/pattern features of the system, giving that individual a consequent face code and the respective synthetic image, allowing the face to identified and recognized at any time with data process methods, because it is compared with this digitalized information of this

person, such that this face code complements the population or census record, or any other kind of specific data base.

7. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with above claims, characterized because the face image of the holder of the identity card, credit card, visa, passport or photograph of a police suspect, is digitalized by scanner/video-camera connected to a computer, where the black/white face image is automatically obtained with 64 to 256 tones of grays, and where an exploration of the face zones is performed using a special image processing computer program, detecting the horizontal zone which gives the maximum frequency of information corresponding to the eye region, where the position of the center point between the rectangular frames of each eye is obtained as central reference point, applying a gradient operator or edge extraction, for example (Sobel) on the virtual face image which is thus obtained, by means of a determinated threshold of grays, where a resulting face image is obtained where the contour edge of the face and the resulting factions/feature of eyes, nose and mouth is represented and where the background of the hair has been suitably filtered and homogenized, such that the system corresponding to the data process program measures, on this virtual face image, the length, width and position of the eyes, nose and mouth.

8. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claim 7, characterized because the data process program extracts the characteristics which distinguish the face features, extracting the most marked edges, comparing the value of each pixel with a reference threshold in respect of the intensity of gray within the information rectangle selected where the eyes, nose, mouth and chin, if applicable, are defined, or else using fuzzy logic/neuronal network technology, the spacial composition and distribution of intensity of grays is determined within the rectangles which frame the eyes, nose and mouth, obtaining space values with respective representation of intensity vectors.

9. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claims 7 and 8, characterized because the master/pattern features contained in the data base on reference features are repeatedly submitted to the process of claims 7 and 8, where for each master/pattern feature, with a master size, their respective characteristic space values are obtained and the respective anthropometric parametric vectors, so that for any face image photograph which is processed in this way, a comparison will be established of its features taken in the form of anthropometric parameters relating to eyes, nose, mouth and chin, as the case may be, obtaining their equivalent master features in the data base on reference features whose most coincident and similar anthropometric parameters are shown in respect of the initial face image and where these master features are printed on the identity card, credit card, visa or passport, by the printer which is connected to the computer, and also the numerical code or colour code corresponding to the selected master features.

10. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claims 7 to 9, characterized because the computer at all times reconstructs and reproduces the face image obtained from the operations corresponding to claims 7, 8 and 9, because a 50 to 100 most significant points of the contour edge of the face and anthropometric parameters are prefixed beforehand, measuring the distance and corresponding angle with the data process program, from the mid-center point of the eyes, obtaining a parametric code of the face image, corresponding to the face of the initial photograph, approximately 400 to 600 characters /Bytes), where these parameters are transmitted by the computer which has generated them, via the conventional transmission line provided with the suitable modem, such that the computer which is located at the other end of this transmission line will receive these characteristic parameters from which it will faithfully reconstruct the initial face image, and where this receiver computer will have the same data base of master/pattern features from which it obtains the master features relating to eyes, nose, mouth and chin, if applicable, corresponding to the code contained in the parameters that have been received,

11. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with above claims, characterized because the respective document, identity card, visa and passport in question as double security validation prints the latent face image of the holder with the bubble jet printer, colour ink injection or by colour sublimation/heat transfer or laser four-chrome printing, electrophotographic printing or photo-electrostatic printing, in colour or black/white tones, connected to the computer where, as an option, the features relating to nose, mouth and eyes of that latent image can be replaced by the selected

master features, so that the composed face image or derived synthetic image can likewise be printed on these documents, made up of the said selected master/pattern features and by the 50 to 100 characteristic parametric points of the face contour-edge which have previously been obtained, printing the numeric code on these documents, as an option, which relates to the master features selected or the colour code corresponding to them, or even both codes.

12. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claim 11, characterized because they include a transparent polyester cover, on whose inner face there is printing with reflector pigment ink and ink visible to UV light, and where a frame is also printed and a crown electric discharge is performed on this inner face, followed straight away by extrusion by hot deposit of a layer of low density polyethylene or polypropylene, placing over the surface which has thus been formed a fine sheet of copper, aluminium or non-thermolaminable plastic, where windows have been performed corresponding to the frames printed on the initial transparent polyester cover, after performing an electric discharge, after which a hot deposit of low density polyethylene or polypropylene is made, as an option with a mixture of collagen/gelatine, to absorb the water soluble ink, after which the sheet is removed from the windows to perform an ink injection print directly on the last surface that has thus been formed, printing grecques, colour watermarks, personal circumstances and face image, and also latent face image and/or composed or synthetic derived face image, foreseeing the option of printing on this surface and also in specular image, the face image, filigrees, grecques, with black/white or colored print, either in an electro-photographic way or else photoelectrostatic way, or with conventional printing.

13. **BIOMETRIC SECURITY AND AUTHENTICATION PROCEDURE FOR IDENTITY AND CREDIT CARDS, VISAS, PASSPORTS AND FACIAL RECOGNITION**, in accordance with claims 11 and 12, characterized because the nucleus of the document is made in white paper, white polyester or some other kind of white plastic, or printing including the option of continuous or complementary or background print lines, with the peculiarity that a crown electric discharge is performed on the surface of both sides, followed by a low density hot polyethylene or polyethylene extrusion which fully thermolaminates in a hot process with the personalized covers of the above claims.

Amended claims

(received by the International Office on 9 August 1995 (09.08.95); claims 1-13 replaced by modified claims 1-13; new claims 14-21 included; (10 pages)

1. Biometric security system for the manufacture of identity cards and credit cards, visas and passports, which starting from the nucleus or support of an identity card or document, with the corresponding personal data and with the face image of the holder transferred to the same, and supported by the use of a color image CCD or line color CCD scanner/video camera connected to its respective computer, essentially characterized in that an exploration is done by means of the scanner, partially or completely digitalizing the surface of the identity document or card,

   - the computer, which embodies a parametrizable algorithm, selecting a sequence of points according to aleatory parameters for each identity document or card, said computer running an analysis for each point chosen, of the colour tone of each one of the points taken from the surface of the card including their face image, likewise assigining to each chosen point with its colour tone a numeric code that, either as numeric code, and printed on the particular card, or in the form of coloured code lines, forming a grecque or filigree the form of a frame or real or virtual code window on the actual card or identity document,
     or, alternately and according to a biometric type,
   - carrying out, by means of the scanner/video camera, an analysis of the face features contained on the identity card or document, the computer carrying out an analysis of the basic features of said image, comparing them with the master/pattern features of a data base and obtaining a series of master/pattern features that correspond to a characteristic synthetic image of that person, printing by the printer connected to the computer, on the virtual or real code window, the coloured lines in form of a grecque or filigree, which univocally characterizes the holder of the cited identity document or card; it optionally being provided for that the resulting numerical code is printed;
     performing said printing by a colour printed connected to the computer, based on a thermal transfer/sublimation technology or cy colour ink injection, electro-photographically or by digital photography.

2. A procedure according to claim 1 characterized in that the computer that embodies a parametrizable algorithm, selects a sequence of points according to

aleatory parameters for each identity card or document, said computer running for each chosen point an analysis of colour tone for each one of the points taken from the surface of the card including the face image, likewise assigning to each chosen point with its colour tone a numeric code that, either as a numerical code, and printed on the particular card, or in the form of coloured code lines, forming a grecque or filigree in the form of a frame or real or virtual code window on the identity card or document itself.

3. A procedure according to claim 1, characterized in that by means of the scanner/video camera, analysis is made of the face features corresponding to the face image contained on the identity card or document, said computer running an analysis of the basic features of said image, comparing them with the master/pattern features of a data base and obtaining a series of standard features that correspond to a synthetic image characteristic of that person, printing with the printer connected to the computer, on the virtual or real code window, the colour lines in form of a grecque or filigree, that univocally characterize the holder of the cited identity card or document; it being provided for that optionally the resulting numeric code is printed.

4. A procedure according to claim 3, characterized in that a series of master/pattern features that form on the screen of the computer a synthetic image characteristic of the person is obtained.

5. A procedure according to any of the above claims, characterized in that the nucleus or support of the identity card or document is provided with colour lines in the form of grecques or filigrees.

6. A procedure according to any of the above claims, characterized in that the Christian name, surnames and birthdate are likewise coded in their equivalency to the corresponding colour code and printed on the real or virtual code window.

7. A procedure according to any of the above claims, characterized in that on the identity card or document a latent image corresponding to the digitalized image of the holder is printed.

8. A procedure according to claim 7, characterized by also printing on the identity card or document the synthetic image or a latent image with certain features replaced by the corresponding master/pattern features.

9. A process for authentication of an identity or credit card, visa or passport carried out according to the procedure according to any of the claims 1-8, characterized in digitalizing by means of a scanner, the real or virtual code window, the code lines of the identity card or document, of whose analysis the computer establishes the equivalency of the colour lines with the master/pattern features to which they correspond, representing on the screen of said computer the synthetic face image corresponding to said master/pattern features, whose synthetic face image should coincide with the facial image of the identity card or document and with the face of the holder of the same.

10. A procedure for authentication according to claim 9, characterized in that it decodes the Christian name, surnames and birthdate.

11. A procedure for authentication of an identity or credit card, visa or passport carried out according to the procedure according to any of the claims 1-8, characterized in that the cited numbering or equivalent of the colour lines of the grecque of window (3) is digitalized by a scanner/video camera and is compared with the resulting code that is to be analysed, by the computer with its facial recognition system, the features of the photo or face image of the card with the master/pattern features that are given rise to, removed from the data base of the master/pattern features, the full coincidence being in that comparison which shows that the card is authentic and the face image of the same thus authenticates the person of the holder.

12. A process for authentication of an identity or credit card, visa or passport carried out according to the procedure according to claim 2, characterized in that exploration is made by the scanner and the digitalization of the lines of the grecque of the real or virtual window of the card code is performed, comparing with the parametrizable algorithm located in the personal computer, whether the set of significant points selected for this card coincides in their resulting numeric code with the equivalent code of the colour lines of the grecque contained in the real or virtual code window,showing the authentiicity or falseness of the card, visa or passport.

13. A procedure of facial recognition characterized in that it comprises

    - comparative data process analysis of an original face image and a data base of master/pattern features, obtaining as a result a numeric code that relates the face image with certain master/pattern features.

14. A procedure of facial recognition according to claim 13, characterized in that the numeric code is printed on the identity document.

15. A procedure for facial recognition according to claim 13 or 14 chracterized in that a synthetic image corresponding to the master/pattern features corresponding to the numeric code is printed on the identity document.

16. A procedure for facial recognition according to any of the claims 13-15, characterized in that it includes live facial recognition with a video camera, or by a photograph digitalized by a scanner, both connected to a computer, of persons that form part of a specific group whose factions have been analyzed and the numeric code corresponding to the master/pattern features corresponding to each person has been obtained, this code being contained in a data base.

17. A procedure for facial recognition according to any of claims 13-16, characterized in that of the live image taken of each person, by a video camera, the basic features of said person are compared by the computer with then master/pattern features of the system, assigning to said person a resulting face code and the corresponding synthetic image, allowing at any moment facial recognition and identification, by data process methods means, of that person, upon being compared with said digitalized information, in such a way that this face code complements the population or census record, or any other type of specific data base.

18. A data processing procedure of face image for use in connection with the procedure according to any of the above claims, characterized in that the face image of the holder of the identity document, credit card, visa, passport or the photograph of a police suspect is digitalized by a scanner/video-camera connected to a computer, automatically obtaining a black/white face image with 64 to 256 tones of gray, where an exploration of the face zones is performed using a special image processing computer program detecting the horizontal zone which gives the maximum frequency of information corresponding to the eye region, where the position of the center point between the rectangular frames of each eye is obtained as a central reference point, applying a gradient operator or edge extraction , for example (Sobel) on the virtual face image which is thus obtained, by means of a determined threshold of grays, where a resulting face image is obtained where the contour edge of the face and the resulting factions/feature of eyes, nose and mouth is represented and where the background of the hair has been suitably filtered and homogenized, such that the system corresponding to the data process program measures, on this virtual face image, the length, width and position of the eyes, nose and mouth.

19. A procedure according to claim 18, characterized in that the data process program extracts the characteristics which distinguish the face features, extracting the most marked edges, comparing the value of each pixel with a reference threshold in respect of the intensity of gray within the information rectangle selected where the eyes, nose, mouth and chin, if applicable, are defined, or else using fuzzy logic/neuronal network technology, the spatial compostion and distribution of intensity of grays is determined within the rectangles which frame the eyes, nose and mouth, obtaining space values with respective representation of intensity vectors.

20. A procedure according to claim 19, characterized in that the master/pattern features contained in the data base on reference features are repeatedly submitted to the process of claims 18 and 19, where for each master/pattern feature, with a master size, their respective characteristics space values are obtained and the respective anthropometric parametric vectors, so that for any face image photograph which is processed in this way, a comparison will be established of its features taken in the form of anthropometric parameters relating to eyes, nose, mouth and chin, as the case may be, obtaining their equivalent master features in the data base on reference features whose most coincident and similar anthropometric parameters are shown in respect of initial face image and where these master features are printed on the identity card, credit card, visa or passport, by the printer which is connected to the computer, and also the numeric code or colour code corresponding to the selected master features.

21. A procedure according to claim 20, characterized in that the computer at all times reconstructs and reproduces the face image obtained from the operations corresponding to claims 18, 19 and 20, because a 50 to 100 most significant points of the contour edge of the face and anthropometric parameters are prefixed beforehand, measuring the distance and corresponding angle with the data process program, from the mid-center point of the eyes, obtaining a parametric code of the face image, corresponding to the face of the initial photograph, by approximately 400 to 600 characters (Bytes), where these parameters are transmitted by the computer which has generated them, via the conventional transmission line provided with the suitable modem, such that the computer which is located at the other end of this transmission line will receive these characteristic parameters from which it will faithfully reconstruct the initial face image, and where this receiver computer will have the same data base of master/pattern features from which it obtains the master features relating to eyes, nose, mouth and chin, if applicable, corresponding to the

code contained in the parameters that have been received.

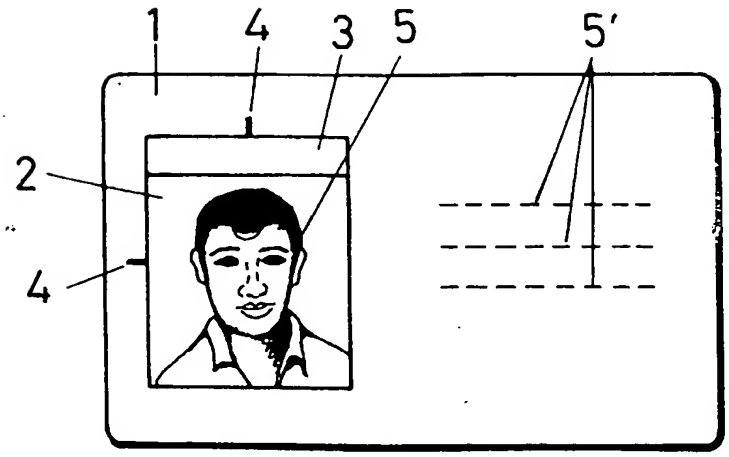

FIG. 1

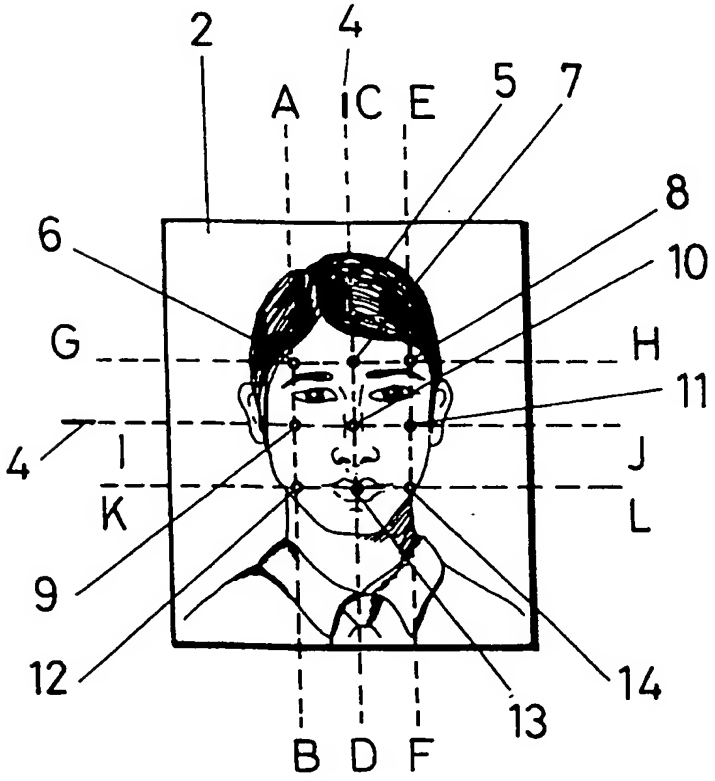

FIG. 2

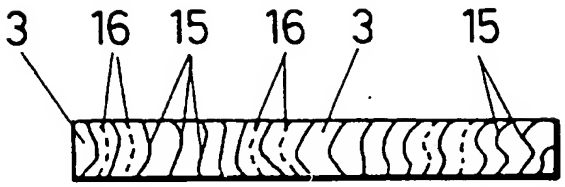

FIG. 3

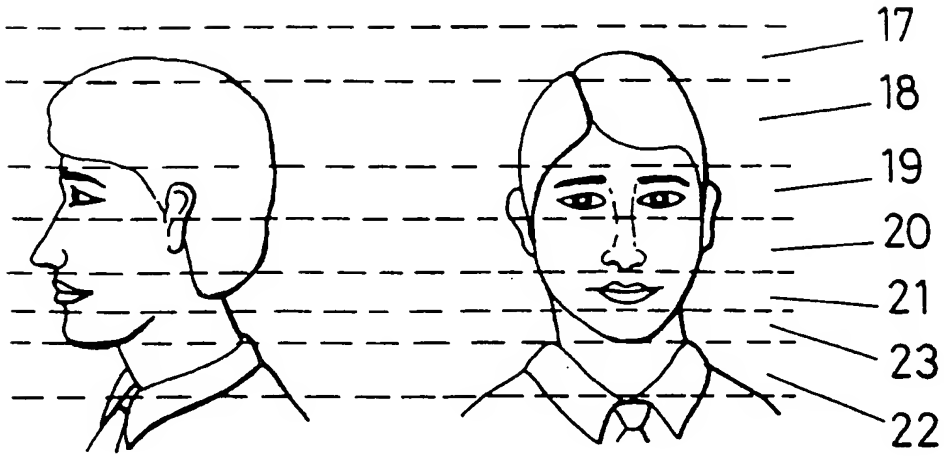

FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/ES 95/00021

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 B42D15/10 G06K9/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K B42D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 440 814 (DAINIPPON PRINTING CO. LTD.) 14 August 1991 see abstract see column 13, line 44 - line 57 see column 14, line 21 - line 37 see column 14, line 48 - column 14, line 33	1,2
Y	US,A,4 975 969 (TAL) 4 December 1990 see abstract see column 2, line 52 - column 3, line 53 see figures 1,2	1-11
Y	US,A,4 972 476 (NATHANS) 20 November 1990 see abstract see column 2, line 37 - column 3, line 6	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 April 1995	04. 08. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	GONZALEZ ORDONEZ, O

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES 95/00021

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE ANNEXED SHEET

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searches without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-11

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1992)

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/ES 95/00021

1. Claims: 1-11 Encoding biometric data on an ID card
2. Claims: 12-13 Materials and method for manufacturing an ID card

1. Independant claim 1 and its dependent claims 2-11 describe a method for the encoding on a data carrier (ID card) of biometric and personal data of a subject in the form of a colour printed pattern and its subsequent decoding and verification.

2. Dependent claims 12 and 13 describe in detail the method and types of materials used for manufacturing the data carrier in its different layers.

There is no common special technical feature linking claims 1-11 to 12 and 13. Consequently the application doesn't comply the requirements of unity of invention (see rule 13 PCT).

The search has been performed, according to Art. 17,3 PCT, on those part of the international application which relate to the invention first mentioned in the claims. (claims 1-11)

Form PCT/ISA.206 (extra sheet) (July 1992)